**Remarks:**

**<u>Status of the Claims</u>**

Claims 1-19 and 61-79 were rejected in the Office Action mailed February 11, 2008. Claim 74 was objected to for the following informality: there appears to be a typo for the word to.

Claims 1, 10, 16, 60, 68, 74 and 76 are amended herein. Claims 1-19 and 61-79 are now pending in the application.

**<u>The Claims</u>**

<u>Claim objection</u>

Claim 74 was objected to for the following informality: there appears to be a typo for the word to. Claim 74 has been amended to correct the typographical error. In light of this correction, Applicants respectfully request that the claim objection to Claim 74 be withdrawn.

**<u>35 USC 112, second paragraph</u>**

Claim 10 was rejected under 35 USC 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner states, "Applicant refers to the at least one state and it is unclear which of the at least one state it is referring to, either the states of the host computer or the software module."

Claim 12 was rejected under 35 USC 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner states, "Applicant claims a Checking RAS state where the RAS is checked if it has data to transmit. It is unclear what a RAS is." Applicants infer that the Examiner intended "12" to refer to "16" as Claim 12 does not refer to RAS whereas Claim 16 appears to contain the objected-to text.

Applicants have amended Claims 10 and 16 (as well as corresponding system claims 68 and 76 that, while not rejected by the Examiner have similar claim language and therefore deemed by the undersigned to merit similar correction) to clarify the subject matter of the invention.

Accordingly, Applicants respectfully request withdrawal of the rejection under 35 USC 112, second paragraph, and the allowance of these Claims.

**35 USC 103**

Claims 1, 18, 61 and 78 were rejected under 35 U.S.C.103 (a) as unpatentable over Urien's US Publication 2003/0086542A1, herein after Urien, in further view of Carper et al. US patent 6,480,935 B1, hereinafter Carper.

Claims 2-17 and 62-77 were rejected under 35 U.S.C.103 (a) as unpatentable over Urien in view of Carper and in further view of Chausset et al's "Serial PC/SC Smart Card Reader Application with TDA8029", hereinafter Chausset.

Claims 19 and 79 were rejected under 35 U.S.C.103 (a) as unpatentable over Urien in view of Carper and in further view of Horiguchi US Publication 2001/0051049 A1, hereinafter Horiguchi.

Applicants traverse these rejections.

Urien is the primary reference cited against the claims and the differences between the claimed invention and Urien are sufficient to overcome these rejections as the other cited references also fail to teach or suggest the limitations from Claims 1 and 61 that are not taught or suggested by Urien. Therefore, to contrast Applicants' claimed invention from that of Urien, Applicants offer the Examiner the following brief summary of Urien and the present application for patent.

Applicants claim a system that allows a resource-constrained device to act as a stand-alone network node that has its own network address. To act as a network node, the resource-constrained device contains an implementation of a communications and network protocol allowing the host computer and remote computers to communicate with the resource-constrained device using those

communications and network protocols. Furthermore, some resource-constrained devices, notably smart cards, are frequently used for implementing security functions, e.g., as part of ensuring transaction security. It is therefore desirable to move the security boundary onto the smart card. i.e., that the host computer to which the resource-constrained device is connected and any intermediate nodes do not need to be trusted because a secure channel has been established from the resource-constrained device to the node with which it communicates securely.

Implementations of security protocols tend to be memory intensive. That presents a problem with implementing such protocols on resource-constrained devices with limited memory, e.g., smart cards. To make such implementations possible applicants have devised clever memory management schemes in conjunction with implementation of security protocols on the smart card.

In contrast, Urien discloses a system in which a host computer and a smart card act together as a network node in which certain data is routed by the host computer to the smart card. Urien discloses what he calls the "smart proxy" (Urien, [0259]). "The smart proxy 27 is embodied by the association of four agents, that is, two in the terminal 1: $T_1$ and $T_2$, and two in the smart card 2a: $S_1$ and $S_2$, and a filter function as described below:" ([0260]). Thus, the "smart proxy", while in some sense a function of the smart card, is a collaboration between the smart card and the terminal.

To allow participation of the smart card in network communications "two specific protocol layers 13 and 23a, respectively, are provided on one hand or other, that is, in the terminal and in the smart card 2a." (Urien, ([0129]). The communication between the smart card and the terminal is according to standard smart card communications protocols as defined by ISO 7816-1 through 7816-4. Furthermore, Urien does not teach or suggest that the smart card has a communications stack that include networking protocols. Rather, Urien uses the standard smart card protocols to carry application level data, e.g., CGI.

**<u>Claim 1 and Claim 61</u>**

Urien fails to teach or suggest, at least, "assigning a network address to the resource-constrained device thereby enabling the resource-constrained device to act as a standalone network node" and "executing on the host computer one or more communication and networking protocols operable to communicate with the resource-constrained device and operable to communicate with the remote network nodes" as recited by Claim 1 (and similarly in Claim 61).

By definition, a smart card does not have the capability of a direct connection to a computer network. Smart cards always connect in some manner via a terminal, often to a host computer, a mobile telephone, or some terminal device. Urien explains this in the context of his invention: "The smart card 2 includes an integrated circuit 20 whose input/output connections … allow a supply of electrical energy and communications with the terminal 1. This terminal includes circuits 11 for access to the internet RI." (Urien, [0069]).

Figures 3 and 5 illustrated the connections between the network, the terminal 1 and the smart card 2a. It is evident from those figures that the card is connected to the terminal which, in turn, is connected to the network.

Given that arrangement, if the card is to have its own IP address, the terminal would have to act as a router of IP communications. However, there is no teaching or suggestion in Urien that the terminal acts as a router.

In Figure 3 Urien illustrates communication protocol layers of the terminal and of the smart card. On the terminal side there "are the upper layers C3 and C4, which correspond to the network addressing (IP, in the case of the internet) and transport (TCP) layers." (Urien, [0121]). There are no counterparts to these layers on the card side.

While Urien's smart card does provide the function of a webserver ([0187]). Urien acknowledges that the functionality cannot be possible directly on the smart card. ([0198]), and explains that the webserver functionality is implemented as sessions between agents([0186] – [0187]). The disclosure of Urien provides an explanation of the pairing of agents on the terminal and smart card, for example, between the web server agent on the smart card and the network agent 132 in the terminal. The agent 132, on the terminal, embodies protocol conversion functions.

Because Urien relies on agents pairs, including one on the terminal and one on the smart card, to cooperate to provide communication with the smart card, there is no need for the TCP/IP layer on the smart card and consequently no need for the smart card to have its own IP address. It is therefore not surprising that Urien fails to teach or suggest "assigning a network address to the resource-constrained device thereby enabling the resource-constrained device to act as a standalone network node" (Claim 1).

Figure 3 of Urien illustrates the communications protocol stacks by which the terminal 1 communicates, on the one hand, to the network, and on the other, to the smart card. "The terminal 1 includes circuits 11 for access to a network" and "software layers C1 and C2, which correspond to physical and data link layers" ([0121]). "Also shown are upper layers C3 and C4, which correspond to the network addressing (IP, in the case of the internet) and transport (TCP) layers. The upper application layer has not been shown." ([0122]). Figure 3 also shows lower layer drivers 15 which are used by the network and transport layers "rest on this interface and are implemented by way of specific function libraries … with which they correspond." ([0123]). Thus, a navigator 10 on the terminal may communicate with a server 4 on the network for applications such as email, web-pages or ftp. ([0124]).

Note that the above describes the communication between the terminal and the network.

The terminal 1 also includes a card reader and card physical (CC1) and data link layers (CC2). These layers implement standard smart card communications protocols defined by ISO standards 7816-1 through 7816-4. ([0125]). An additional software layer 16 forms an interface between the application layers and the lower layers CC1 and CC2. <u>"In accordance with the invention, two specific protocol layers 13 and 23a, respectively, are provided on one hand and other , that is, in the terminal and in the smart card 2a."</u> ([0129]). <u>"In the terminal 1, the specific layer 13 interfaces with 'low driver layers' 15, libraries 14 of network layers C3 and C4, and protocol layers for the card reader 3, that is, the lower layers CC1 and CC2, via the multiplexing layer 16. The specific layer 13 enables the transfer of network packets</u>

from and to the smart card 2a. It also adapts the existing applications, such as the internet navigator 10, email, etc., for uses that employ the smart card." ([0130]).

Thus, communication between the network and the smart card, according to Urien, is via a specific layer 13.

There is a corresponding organization on the smart card including a specific layer 23a which is a counterpart of the layer 13. ([0131]).

The two corresponding layers have three principal software elements: a module 130 and 130a for transferring blocks of information via the conventional layers CC1, CC2 (on the terminal) and CCa1 and CCa2 (on the smart card), intelligent agents that perform protocol conversion functions, and configuration management. ([0132] – [0135]).

As discussed above, communication between the terminal 1 and the smart card is by way of pairs of agents that are implemented above the physical link and data link layers connecting the terminal to the smart card. Within the specific layers 13 and 23a there are pairs of cooperating agents, *viz*., "the first agent of each pair, 132, is located in the layer 13 of the terminal 1, while the second agent, 232a, is located in the layer 23a in the smart card 2a." ([0147]). "A link between two agents is associated with a session that will be called 'S-agent''. A session is a bidirectional data exchange between these two agents." ([0147]).

Urien discloses that the terminal implements two stacks on the terminal, one for communicating with the network and another for communicating with the card. ([0184]). The first stack contains network and protocol layers (TCP/IP). The other stack contains ISO 7816-3 (C1 and C2), APDU (i.e., ISO 7816-4), and a packet multiplexer 130.

To make the smart card operate as a client/web server by implementing sessions between agents. ([0187]). Thus, communication between the network and the card requires active cooperation with the terminal.

While Urien discloses that the webserver function offered by Urien's smart card includes a mechanism similar in function to CGI (Common Gateway Interface) ([0191]), after describing CGI ([0192]-[0197]), Urien concedes that "[that] mechanism cannot, however, be transposed directly to a smart card, even if the smart

card has the client/webserver function in accordance with one of the characteristics of the invention. To perform that, Urien relies on agents called script translator agents. ([0200] through [0207]). A script translator agent generates a set of APDU orders. "A session is opened between the translator agent, such as the ATSi and the APDU agent 2101a [on the card]. The orders are then sent to the APDU agent 2101a. The APDU order manager 210a selects the GCA [General Card Application] Ai and sends it the APDU orders." ([0208]). It should be noted that Urien describes the GCAs as being unmodified smart card applications. ([0090]).

In other words, the translator agent, which operates on the terminal, makes a translation from the web application protocol into APDU. The terminal through the 7816-4 and 7816-3 terminal-to-smart card protocols communicate this APDU which is then serviced by a smart card application in a traditional smart card way of command-response. Since the communication to the smart card applications is in the way of APDU, there is no need for the smart card of Urien to implement a TCP/IP stack. Hence, it is not surprising to find that Urien does not teach or suggest "executing on the resource-constrained device a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with a host computer, operable to communicate with remote network nodes using the networking protocols and operable to implement network security protocols thereby setting a security boundary inside the resource-constrained device" (Claim 1).

From the foregoing it is not surprising that Urien fails to teach or suggest "executing on the host computer one or more communication and networking protocols operable to communicate with the resource-constrained device and operable to communicate with the remote network nodes"(Claim 1) because Urien teaches a system that relies on transmission of application data via APDU to the smart card without establishing a direct TCP/IP connection to the card. While Urien describes a system in which the smart card may execute certain web applications, e.g., CGI, the communication between Urien's card and the remote network node is not via network communication that originates and terminates, respectively, on the smart card.

Claim 1 further recites "implementing an execution model, wherein the communication module is driven by input events and by the applications and wherein the resource-constrained device optimized memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers" (Claim 61 has a similar limitation). Urien does not teach or suggest this element and the Examiner has not alleged anything to that effect.

Carper does teach memory management techniques for smart cards. However, Carper does not teach or suggest sharing data buffers between communications protocol layers and security protocol layers. Considering that Urien fails to teach or suggest the implementation of communications protocol layers on the smart card (see above) and Carper does not either, it follows that a combination of Urien and Caper would similarly fail to have such feature. Accordingly, the combination of Urien and Carper does not provide a method for communication between a smart card and remote network nodes with the limitation of "implementing an execution model, wherein the communication module is driven by input events and by the applications and wherein the resource-constrained device optimized memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers."

For the foregoing reasons, Claims 1 and 61 (having similar limitations as those argued above in support of Claim 1) are patentable over Urien.

Carper similarly does not teach or suggest the limitations argued above with respect Urien. Carper teaches a smart card memory manager. But does not teach or suggest any of the limitations set forth in Claims 1 and 61 that differentiate those claims from Urien. Therefore, a combination of Urien and Carper would fail to teach or suggest the invention set forth in Claims 1 and 61.

**<u>Claims 2-19 and Claims 62-79</u>**

Chausset discloses a smart card coupler. Horiguchi teaches a digital camera that includes a multi-media card. However, Carper, Chausset, and Horiguchi all do not deal with data communication with a smart card using networking technology. Therefore it is not surprising that these references fail to teach or suggest the

limitations discussed herein above in support of Claims 1 and 61. Accordingly, Claims 1 and 61 are patentable over any combination of these cited references.

Claims 2-19 are all dependant claims deriving from Claim 1, incorporate the limitation of Claim 1, provide further unique and non-obvious combinations, and are therefore patentable over Urien for, at least, the reasons given in support of Claim 1 and by virtue of such further combinations.

Claims 62-79 are all dependant claims deriving from Claim 61, incorporate the limitation of Claim 61, provide further unique and non-obvious combinations, and are therefore patentable over Urien for, at least, the reasons given in support of Claim 61 and by virtue of such further combinations.

## CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: June 30, 2008

/Pehr Jansson/
Pehr Jansson

Registration No. 35,759

The Jansson Firm
9501 N. Capital of Texas Hwy #202
Austin, TX 78759
512-372-8440
512-597-0639 (Fax)
pehr@thejanssonfirm.com